SICUREZZA CON SSL/TLS

La sicurezza delle connessioni con SSL/TLS è un protocollo crittografico utilizzato per garantire la sicurezza delle comunicazioni tra client e server su Internet. SSL (Secure Sockets Layer) è stato il primo protocollo di sicurezza a essere utilizzato, ma è stato sostituito da TLS (Transport Layer Security) che è più sicuro.

SSL/TLS utilizza un sistema di crittografia a chiave pubblica per garantire che i dati scambiati tra il client e il server siano protetti da terze parti. In particolare, il client e il server stabiliscono una connessione crittografata utilizzando un certificato digitale rilasciato da un'autorità di certificazione.

Secure Socket Layer (SSL) ⇒ sicurezza a livello SESSIONE (OSI) con funzionalità di cifratura ed autenticazione DES ed RSA

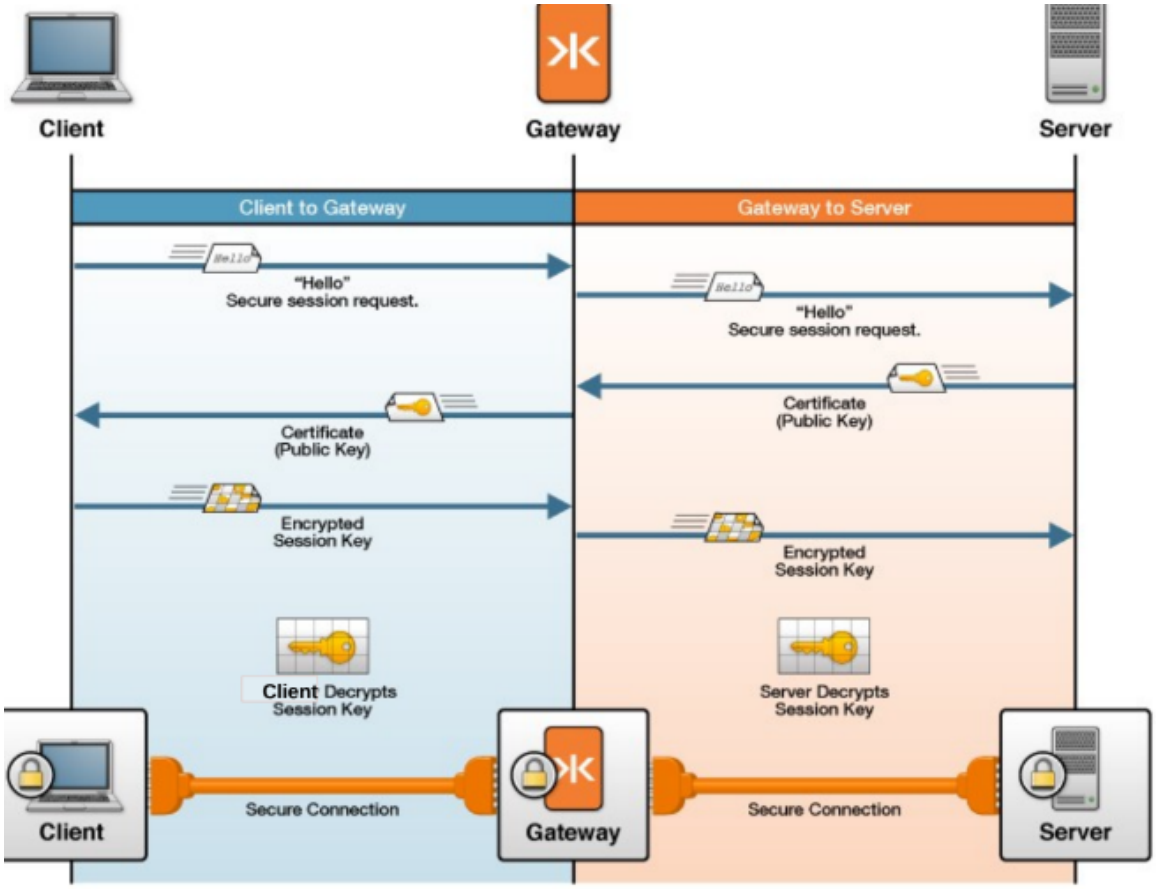
EVOLUZIONE:

1. Nasce come SSL con il browser Netscape Navigator (antesignano di Mozilla-Firefox).
2. Si evolve con SSL/TLS, protocollo standardizzato come Trasport Layer Security fra client e server certificati.
    - HTTPS: Combinazione di http con SSL-TLS (porta 443).
    - S-HTTP: Incapsulamento messaggi crittografati in formato MIME/CMS.
    - SMTPS :465 POPS :995 IMAPS :993 Combinazione con gli standard di invio/ricezione messaggi di posta elettronica.

Funzionamento del TLS:

- TLS record protocol: Opera appena sopra il livello trasporto affidabile (TCP), suddividendo in blocchi i dati del livello superiore, calcolando il MAC e cifrando.

- TLS handshake protocol: Opera nella fase di negoziazione della connessione e si divide in:
  - Handshake protocol: Instaurazione connessione.
  - Change chiper spec: Scambio chiavi e certificati fra client e server.
  - Alert protocol: Segnala problemi nella sessione SSL.



La fase di definizione della session key si divide prevede premaster key generata dal client grazie al certificato che contiene la chiave pubblica e quindi la decifrazione della chiave di sessione da parte del server con la sua chiave privata.